U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF THE SECRETARY

DOT H 1350.257
May 21, 1999

DEPARTMENTAL GUIDE TO PHYSICAL/ENVIRONMENTAL SECURITY PLANNING

TABLE OF CONTENTS

DEPARTMENTAL GUIDE
TO
PHYSICAL/ENVIRONMENTAL SECURITY PLANNING

1. PURPOSE

The purpose of this Guide is to provide Department of Transportation (DOT) and their Operating Administration managers, ISSO's and network administrators with a step-by-step approach for developing both a physical and environmental security capability within their organizations.

2. SCOPE

The provisions of this Guide apply to the Department of Transportation (DOT), its Secretarial Offices and Operating Administrations.

3. GOALS

The Goal of physical/environmental security planning is to provide protection for the DOT facility housing information system resources, the system resources themselves, and the facilities used to support their operation.

4. REFERENCES

The DOT Departmental Information Resources Management Manual (DIRMM) DOT H 1350.2 implements statutory and regulatory Information Resources Management (IRM) and security requirements for the Department. It also calls for ensuring the confidentiality, integrity, and availability of information contained, processed, or transmitted in/on sensitive systems. Refer to DOT H 1350.2.1 Regulatory and Guidance Documents for specific references.

5. OVERVIEW OF PHYSICAL/ENVIRONMENTAL SECURITY

Physical/Environmental Security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Such threats, and the measures taken to mitigate them, depend on three sets of characteristics:

- <u>Physical Characteristics</u> – The basic physical characteristics of the DOT facility housing the information system or systems determine the level of such physical threats as fire, roof leaks, or unauthorized access. In particular, whether the facility is fixed (e.g., a building), or mobile (e.g., an airplane) is of particular significance in terms of deriving the appropriate security measures.
- <u>Geographical Characteristics</u> – The particular location of the DOT facility housing the information system or systems determines the characteristics of natural threats (including earthquakes and flooding), man-made threats (such as burglary, civil disorders, or interception of transmissions and emanations), and damaging nearby activities (including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters such as radar).
- <u>Characteristics of Supporting Facilities</u> – The operation of DOT information systems usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and may cause physical damage to system hardware or stored data.

Properly applied, Physical/Environmental security controls can prevent losses due to interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft. These Physical/Environmental security controls encompasses seven primary areas:

1) **Physical Access Controls**

Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a local area network (LAN) server.

2) **Fire Safety Controls**

Building fires are a particularly important security threat because of the potential for complete destruction of hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Fire safety controls guard against the start of fires, ensure early detection should a fire start, and assist in rapid fire extinguishing.

3) **Protecting Supporting Utilities**

A failure of electric power, heating or air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage system hardware. Systems and the people who operate them therefore need to have a reasonably well-controlled operating environment, with appropriate safeguards that would mitigate such failures.

4) **Preventing Structural Collapse**

Buildings housing information systems may be subjected to a load greater than they can support. Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members.

5) **Preventing Plumbing Leaks**

Plumbing leaks are not an everyday occurrence. However, should such a leak occur, the resulting water damage could seriously disrupt facility operations.

6) **Guarding Against Interception of Data**

Depending on the type of data processed by an information system, there may be a significant risk if that data is intercepted. There are three primary methods of data interception: direct observation, interception of data transmission, and electromagnetic interception.

7) **Protecting Mobile and Portable Systems**

The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks.

6. PHYSICAL ACCESS CONTROLS

Issues to be considered in deriving a set of physical access controls include:

- Addressing physical access controls not only the for areas containing system hardware, but also for locations containing wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.
- Considering both normal access and surreptitious access when evaluating methods for restricting physical access. Restricting normal access may include barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points (e.g., badges or card-key devices). Physical modifications to barriers can reduce the vulnerability to surreptitious entry. Intrusion detectors, such as closed-circuit television cameras, motion detectors, and other devices, can detect intruders in unoccupied spaces.
- Using DOT employees. Staff members who work in a restricted area can serve an important role in providing physical security, as they can be trained to challenge people they do not recognize.
- Ensuring that maintenance and service personnel are properly escorted and supervised by a DOT employee with enough background, training or qualifications to understand the risks associated with the work being done, and provide assurance that only authorized access to sensitive information or assets takes place.
- Ensuring that signs or other information revealing the purpose or location of restricted zones as they relate to sensitive information systems are not posted in areas accessible to the general public such as lobbies, waiting rooms or reception areas.
- Remembering that physical and environmental controls are also closely linked to the activities of the local guard force, fire house, life safety office, and medical office. These organizations should be consulted for their expertise in planning controls for the information systems environment.

In addition, it is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied. Effectiveness depends on both the characteristics of the control devices used (e.g., keycard-controlled doors) and the implementation and operation. Statements to the effect that "only authorized persons may enter this area" are not particularly effective. Organizations should determine whether intruders can easily defeat the controls, the extent to which strangers are challenged, and the effectiveness of other control procedures. Factors like these modify the effectiveness of physical access controls.

7. FIRE SAFETY CONTROLS

Issues to be considered in developing plans for fire safety controls include:

- Identifying and neutralizing potential ignition sources. Fires begin because something supplies enough heat to cause other materials to burn. Typical ignition sources are failures of electric devices and wiring, carelessly discarded cigarettes, improper storage of materials subject to spontaneous combustion, improper operation of heating devices, and, of course, arson.
- Isolating and properly storing potential fuel sources. If a fire is to grow, it must have a supply of fuel, material that will burn to support its growth, and an adequate supply of oxygen. Once a fire becomes established, it depends on the combustible materials in the facility (referred to as the fire load) to support its further growth. The more fuel per square meter, the more intense the fire will be. In addition, if the facility is well maintained and operated so as to minimize the accumulation of fuel sources, the fire risk will be further minimized.

- Planning for reliable, effective means of fire detection. The more quickly a fire is detected, all other things being equal, the more easily it can be extinguished, thereby minimizing damage to the facility. It is also important to accurately pinpoint the location of the fire.
- Providing rapid access to sufficient means of fire extinguishment. A fire will burn until it consumes all of the fuel in the building or until it is extinguished. Fire extinguishment may be automatic, as with an automatic sprinkler system or a chemical discharge system. Alternatively, it may be performed by people using portable extinguishers, cooling the fire site with a stream of water, limiting the supply of oxygen with a blanket of foam or powder, or breaking the combustion chemical reaction chain.

8. PROTECTING SUPPORTING UTILITIES

Issues to be considered in developing plans for protecting utilities that support an organization's information systems include:

- Identifying the failure modes of each utility (air conditioning, electric power distribution, heating plants, water, sewage, and other utilities) required for system operation or staff comfort.
- Calculating the Mean Time Between Failure (MTBF) for each major element comprising these utilities. This serves as an indicator for how often to expect a failure that could affect facility operations. If the results are unacceptable, consider ways to either replace high MTBF items with more reliable ones (cost permitting), or stock an adequate level of spares.
- Calculating the Mean Time To Repair (MTTR) for each major element. Remember, until the utility is repaired, users may be denied access to vital information system data, or be without important communication links. Consider added training for maintenance personnel, or pre-positioned spares to reduce MTTR if possible.
- Determining the need for dual-redundant or backup utilities for critical system support (such as Uninterruptable Power Supplies).
- Ensuring that emergency lighting exists in computer rooms.
- Ensuring that supporting utilities such as power distribution panels, communications and telephone closets, and air conditioning systems, when located outside restricted zones established within the facility are appropriately secured by such measures as locks.
- Considering the screening or filtering of external openings for air conditioning systems to protect against the insertion of hazardous objects or the intrusion of pollutants.
- Ensuring, if possible, that utility service lines (water, gas, oil, etc.) that provide support to facilities enter the building underground or are physically protected by other means, such as enclosing exposed lines in conduit, installing barriers around water and gas mains or meters, and locking fuel tank inlet pipes.

9. PREVENTING STRUCTURAL COLLAPSE

Issues to be considered in developing plans for preventing the structural collapse of an organization's facility include:

- Determining, for a building in the construction planning stage, the likelihood of structural collapse due to environmental factors such as an earthquake or snow load and, if probabilities warrant, ensuring that adequate precautions are taken regarding structural design strengths.
- Determining, for a building in the construction planning stage, the likelihood of structural collapse due to natural or man-made disasters, such as a major fire, gas explosion or sabotage, again ensuring that adequate precautions are taken regarding structural design strengths.
- Determining, for an existing building, the likelihood that of any of these factors could result in structural collapse, given the existing facility design. If probabilities and design weaknesses warrant, consider, --- at a minimum, --- Continuity Of Operations (COOP) planning that incorporates hot or cold site utilization (refer to DOT H 1350.254 *Departmental Guide to*

Continuity of Operations Planning). In the worst case, a change of facilities should be seriously considered.

10. PREVENTING PLUMBING LEAKS

Issues to be considered in developing plans for preventing plumbing leaks include:

- Locating plumbing lines that might endanger system hardware. These lines include hot and cold water, chilled water supply and return lines, steam lines, automatic sprinkler lines, fire hose standpipes, and drains. If a building includes a laboratory or manufacturing spaces, there may be other lines that conduct water, corrosive or toxic chemicals, or gases.
- Considering the relocation of potentially damaging lines. As a rule, analysis often shows that the cost to relocate threatening lines is difficult to justify. However, the location of shutoff valves and procedures that should be followed in the event of a failure must be specified. Operating and security personnel should have this information immediately available for use in an emergency. In some cases, it may be possible to relocate system hardware, particularly distributed LAN hardware.

11. GUARDING AGAINST INTERCEPTION OF DATA

Issues to be considered in developing plans for guarding against the interception of data include:

- Eliminating problems due to direct observation, whereby system terminal and workstation display screens may be observed by unauthorized persons, by relocating susceptible displays.
- Guarding against interception of data transmissions. If an intruder can gain access to data transmission lines, it may be feasible to tap into the lines and read the data being transmitted. Network monitoring tools can be used to capture data packets. Of course, the intruder cannot control what is transmitted, and so may not be able to immediately observe data of interest. However, over a period of time there may be a serious level of disclosure. Local area networks typically broadcast messages. Consequently, all traffic, including passwords, could be retrieved. Interceptors could also transmit spurious data on tapped lines, either for purposes of disruption or for fraud.
- Preventing electromagnetic interception. Systems routinely radiate electromagnetic energy that can be detected with special-purpose radio receivers. Successful interception depends on the signal strength at the receiver location; the greater the separation between the system and the receiver, the lower the success rate. TEMPEST shielding, of either equipment or rooms, can be used to minimize the spread of electromagnetic signals. The signal-to-noise ratio at the receiver, determined in part by the number of competing emitters will also affect the success rate. The more workstations of the same type in the same location performing "random" activity, the more difficult it is to intercept a given workstation's radiation. On the other hand, the trend toward wireless (i.e., deliberate radiation) LAN connections may increase the likelihood of successful interception.

12. PROTECTING PORTABLE AND MOBILE SYSTEMS

Issues to be considered in developing plans for protecting portable and mobile systems include:

- Guarding against compromise or damage due to accident or theft of the system’s means of transport (e.g., automobile, truck, airplane).
- Guarding against theft of portable and mobile systems. As they tend to be small and relatively lightweight, they share an increased risk of theft. In addition, portable systems can be "misplaced", damaged or left unattended by careless users. Secure storage of laptop computers is often required when they are not in use.
- Considering storing valuable or important data on a medium that can be removed from the portable/mobile system when it is unattended, or to encrypt the data.